AFFIDAVIT

I, Michael D. Fleener, being duly sworn, do hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the U.S. Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI"), and have been so employed since April 2001. I am currently assigned to the Office of the Resident Agent in Charge, in Charleston, West Virginia. Prior to becoming a Special Agent, I was employed as a police officer in Lexington, Kentucky, from July 1995 to March 2001. I also served in the United States Marine Corps as a military police officer from April 1990 to July 1995. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. For the past 15 years, I have investigated violations of federal law including the online exploitation of minors, particularly in relation to violations of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422(b). I have participated in the execution of search warrants involving child exploitation and child pornography offenses, and the search and seizure of computers and other digital devices related to those offenses. I am a member of the West Virginia Internet Crimes Against Children ("WV ICAC") Task Force and work with other federal, state, and local law enforcement personnel in the

investigation of crimes involving the sexual exploitation of children.

II. PURPOSE OF THE AFFIDAVIT

2. The statements contained in this affidavit are based on my knowledge or information provided by Facebook and the National Center for Missing and Exploited Children. This affidavit is being submitted for the limited purpose of securing a search warrant. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause that violations of Title 18, United States Code, Sections 2251(a), (c) and (e) (production and attempted production of child pornography); 2252(a)(1) and (b)(1) (transportation of a visual depiction of a minor engaged in sexually explicit conduct); 2252(a)(2) and (b)(1) (receipt and distribution of a visual depiction of a minor engaged in sexually explicit conduct); 2252A(a)(1) and (b)(1) (transportation of child pornography); 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography); 2252A(a)(5)(B) and (b)(2) (possession and access with intent to view child pornography); and 2422(b) (coercion and enticement of a minor) have occurred in Boone County, West Virginia, within the Southern District of West Virginia, and that evidence of those violations is located on CDs currently located at HSI Charleston, 210 Kanawha Blvd. W, Charleston, WV

25302, which were submitted by Facebook as part of the associated CyberTip Reports 15070021, 15197258 and 15250552.

III. STATUTORY AUTHORITY

3. The investigation concerns violations of 18 U.S.C. §§ 2251, 2252, 2252A and 2422(b) relating to matters involving the sexual exploitation of minors.

a. 18 U.S.C. § 2251 prohibits any person from employing, using, persuading, inducing, enticing or coercing any minor to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, or for the purpose of transmitting a live visual depiction produced using materials that had traveled in interstate commerce or transported in or affecting interstate commerce.

b. 18 U.S.C. § 2252(a)(1) prohibits any person from knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of a minor engaging in sexually explicit conduct.

c. 18 U.S.C. § 2252(a)(2) prohibits any person from knowingly receiving or distributing, by computer or mail, any visual depiction of a minor engaging in sexually explicit conduct that has been mailed or shipped or transported in interstate or foreign commerce. That section also makes it a Federal crime for any person to knowingly reproduce any visual depiction of a minor engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.

d. 18 U.S.C. § 2252A(a)(1) prohibits any person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. § 2252A(a)(2) prohibits any person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. § 2252A(a)(5)(B) prohibits any person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

g. 18 U.S.C. § 2422(b) prohibits any person from using the mail or any facility or means of interstate or foreign commerce to knowingly persuade, induce, entice or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempting to do so.

4. The following definitions apply to this Affidavit and its Attachments.

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where

i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether

in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact disks, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-locations of computers and other communications equipment.

h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static if an ISP assigns a user's computer a particular IP address each time the computer accesses the Internet.

i. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of www.usdoj.gov refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

k. A "Preservation Letter" is a letter governmental entities may issue to Internet providers pursuant to 18 U.S.C. § 2703(f) to ensure that the Internet Providers preserve records in their possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted.

IV. BACKGROUND REGARDING COMPUTERS, THE INTERNET AND EMAIL

5. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skill were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute

these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.[1] Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of

[1] The File Transfer Protocol ("FTP") is a protocol that defines how files are transferred from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

distribution and receipt of child pornographic materials among pornographers.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc. and Google, Inc., among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic

communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on the computer indefinitely until overwritten by other data.

V. BACKGROUND ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN'S CYBERTIPLINE

6. Based on my training and experience, and publicly-available information, I know that the National Center for Missing and Exploited Children ("NCMEC") is a nonprofit, nongovernmental organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

7. In addition to reports from the general public, Title 18, United States Code, Section 2258A requires all providers of an electronic communication service or remote computing service to the public through a facility or means of interstate or foreign commerce, to report "apparent child pornography" to NCMEC via the CyberTipline. Leads are reviewed by specially-trained analysts,

who examine and evaluate the reported content, add related information that may be useful to law enforcement, use publicly-available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

8. The CyberTipline receives reports, known as CyberTip Reports, on the following type of criminal conduct: possession, manufacture and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

9. The CyberTip Reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an electronic communication service or remote commuting service uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip

code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography. See 18 U.S.C. § 2258A(b). Also, as will be illustrated below, CyberTip Reports can be supplemented and made in connection with other CyberTip Reports.

VI. BACKGROUND ON FACEBOOK

10. Facebook owns and operates a free-access social networking website of the same name, accessible at http://www.facebook.com. Facebook allows users to create personal accounts by which they can upload and share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

11. In order to create an account, Facebook requires users to provide basic contact and personal identifying information, such as first and last name, birth date, gender, and contact e-mail address or mobile number. Users must also create an account password and answer security questions (for password retrieval). Once an account is successfully created, Facebook assigns the account a user identification number ("UIN").

12. Facebook users may join one or more groups or networks to connect and interact with other users. Facebook assigns a group identification number to each group. A Facebook user may also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient accepts the request,

then the two users will become "Friends" and can exchange communications or view one another's information. Each Facebook user account includes a list of "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, recent posts or upcoming events.

13. Facebook users can select different levels of privacy for the communications and information associated with their accounts. By adjusting these privacy settings, a user can set their account to completely private, to accessible only to particular Facebook users, or accessible to anyone, including people who are not Facebook users. Users can also limit the types of notifications they receive, by clicking the "Friends" tab to adjust these privacy settings.

14. Facebook users can create profiles that include photographs, personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their whereabouts at particular dates and times. A particular user's profile page also includes a "Wall,"

which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone allowed access to the user's page.

15. Facebook allows users to upload photos and videos, which may include metadata such as the location where the photo or video was uploaded. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged, he or she receives a notification of the tag and a link to the upload. The photos and videos associated with a user's account, including those tagged, remain accessible unless/until deleted.

16. Facebook users can also exchange private messages. These messages, which are similar to e-mail messages, are sent to the recipient's "page." Copies of messages sent to/by the recipient are retained on Facebook. Facebook users can also post comments to their page of other's pages; such comments are typically associated with a specific posting or item on the page. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history of each account. Facebook also has a Video Calling feature, and although Facebook does not record the actual calls, it does keep a record of the date and time of each call.

17. If a Facebook user chooses not to interact with another particular user, the first user can "block" the second user from seeing the contents of his or her page.

18. Facebook has feedback options which allow users to "like," comment or share particular posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites.

19. Facebook has a search function that enables users to search Facebook for keywords, usernames, or pages, among other things.

20. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities occurring from the inception of the account to the present. The activity log includes photos or events that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by others who may visit the user's page.

21. Facebook Notes is a feature which enables users to write and post notes or personal web logs ("blogs"), or to import blogs from other services, such as Xanga, LiveJournal, and Blogger to their page.

22. The Facebook Gifts feature allows users to purchase and send virtual "gifts" along with a personal message to other users which appear as icons on the recipient's profile page. Facebook

users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

23. Facebook also has a Marketplace feature, which allows users to post free classified ads, such as items for sale, housing or jobs. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, a notification of such may appear on the user's profile page.

VII. FACTS ESTABLISHING PROBABLE CAUSE

24. On or about October 21, 2016, Facebook submitted CyberTip Report 15070021 to the NCMEC CyberTipline. The Cybertip Report was the result of Facebook representatives visibly identifying an image file. The Cybertip Report indicated that the reporting electronic communication service provider, i.e., Facebook, viewed the entire contents of the image file depicting a minor's naked breasts. The image was allegedly sent via private message from one Facebook user who claimed to be 13 years of age, to another Facebook user.

25. On or about October 29, 2016, Facebook submitted CyberTip Report 15197258 to the NCMEC CyberTipline. The CyberTip Report was the result of Facebook representatives visibly identifying 14 image files they believe contained child pornography. The Cybertip

Report indicated that the reporting electronic communication service provider, i.e., Facebook, viewed the entire contents of two of the 14 image files uploaded. These image files were identified as alphanumeric file _123082144_n.jpg and alphanumeric file _2092700697_n.jpg., and depict an apparent female minor's naked breasts and vagina. Facebook did not view the entire contents of the other 12 image files. These 12 image files are contained on a CD which was attached to CyberTip Report 15197258.

26. According to Facebook, the 14 image files were sent between October 24, and October 26, 2016, by a Facebook user with the screen/user name: akers.marty.7., to a Facebook user with the screen/user name: ashley.boone.984991. Your affiant recently confirmed through Facebook representatives that both of these accounts appear to have been created and utilized by Marty Akers.

27. On or about November 2, 2016, Facebook submitted CyberTip Report 15250552 to the NCMEC CyberTipline. The report was the result of Facebook representatives' concern over possible online enticement. The report revealed that Marty Akers has at least two Facebook accounts which he uses to communicate with minors. According to the report, Marty Akers obtained a photo depicting apparent child pornography from child victim #1 on or about September 3, 2016. He then sent that photo to his Facebook account with the screen/user name: ashley.boone.984991. Specifically, the CyberTip Report documents two Facebook

conversations between Marty Akers and two female minors, wherein Marty Akers engaged in sexually explicit conversations with the two female minors and enticed one female minor to produce and send the apparent child pornography image of herself. The CyberTip Report further provided the following Facebook accounts registered to Marty Akers: DOB: [redacted]-1981; screen/user name: akers.marty.7; with an email address: martyakers2424@gmail.com., as well as screen/user name: Ashley.boone.984991 with email address ashboone24@outlook.com. Both accounts were accessed between October 27-28, 2016 from the same IP address 104.218.186.172.

28. Facebook representatives indicated that all three submitted CyberTip Reports relate to the same Facebook user, Marty Akers. Your affiant recently confirmed that Marty Akers, with date of birth of [redacted]1981, currently resides at [redacted] Josephine Avenue, Madison, Boone County, West Virginia.

29. Your affiant, who has been actively investigating child exploitation for the past 15 years as an HSI Special Agent, has routinely received and investigated dozens of CyberTip Reports from NCMEC. As such, I am aware of the federal district court decision in United States v. Keith, 980 F. Supp. 2d 33 (D. Mass. 2013). In that case, the court held that the NCMEC acted as a government agent when a NCMEC analyst opened and viewed an electronic mail attachment that an Internet Service Provider had forwarded to the NCMEC as suspected child pornography, without a

search warrant, in violation of the Fourth Amendment. Id. at *12. Although Keith is not controlling in this district and there is reason to question its reasoning, in an abundance of caution, your affiant did not view the 12 image files referenced herein which were not viewed in their entirety by Facebook.

30. Your affiant knows through experience investigating dozens of CyberTip Reports over the past fifteen years that, in every case, the CyberTip Report contains information and/or evidence of child exploitation either in image files, video files or captured conversations between a victim and a reported subject.

VIII. CONCLUSION

31. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that the "unviewed" attachments submitted by Facebook, as part of the associated CyberTip Report 15197258, received by NCMEC on October 29, 2016, contain evidence of criminal offenses, namely Title 18, United States Code, Sections 2252, 2252A, and 2422 (b).

32. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the CD described in Attachment A which is currently in the care, custody and control of your affiant and HSI, located at 210 Kanawha Blvd. W, Charleston, West Virginia, within the Southern District of West Virginia.

SPECIAL AGENT MICHAEL D. FLEENER
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

Subscribed and sworn before me this the 1st day of December, 2016.

DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE